UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA

KELLI GIPSON and ALYSSA GASEOR, on behalf of themselves and all others similarly situated, Plaintiffs, v. **DUKE ENERGY CORPORATION,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Kelli Gipson and Alyssa Gaseor ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Duke Energy Corporation ("DEC" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against DEC for its failure to properly secure and safeguard Plaintiffs' and other similarly situated DEC customers' name, date of birth, last four digits of Social Security number and/or federal tax ID number, account numbers, property or mailing addresses, meter serial numbers, email addresses, and phone numbers (the "Private Information") from hackers.

2. DEC, based in Charlotte, North Carolina, is one of America's largest energy holding companies that serves more than 8 million customers in seven states.[1]

3. On or about December 12, 2024, DEC sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

4. Based on the Notice, DEC detected unusual activity on some of its computer systems in May 2024. In response, the company conducted an investigation which revealed that an unauthorized party had access to certain company files between May 20, 2024, and May 24, 2024 (the "Data Breach"). Yet, DEC waited roughly seven months to notify the public that they were at risk.

5. As a result of this delayed response, Plaintiffs and "Class Members" (defined below) had no idea for almost seven months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

6. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, last four digits of Social Security number and/or federal tax ID number, account numbers, property or mailing addresses, meter serial numbers, email addresses, and phone numbers that DEC collected and maintained.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining

[1] See https://www.duke-energy.com/our-company/about-us (last visited Dec. 23, 2024).

driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by DEC that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs bring this class action lawsuit to address DEC's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

11. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to DEC, and thus DEC was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

12. Upon information and belief, DEC and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had DEC properly monitored its networks, it would have discovered the Breach sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of DEC's negligent conduct as the Private Information that DEC collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

16. Plaintiff Kelli Gipson is, and at all times mentioned herein was, an individual citizen of the State of North Carolina.

17. Plaintiff Alyssa Gaseor is, and at all times mentioned herein was, an individual citizen of the State of Florida.

18. Defendant Duke Energy Corporation is an American electric power and natural gas holding company headquartered in Charlotte, North Carolina, having its principal place of business located at 525 S Tryon St, Charlotte, North Carolina 28202.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from DEC. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over DEC because DEC operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and DEC has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. DEC's Business and Collection of Plaintiffs' and Class Members' Private Information

22. DEC is an American electric power and natural gas holding company. Founded in 1904, DEC is a fortune 150 company that provides electric services to "8.4 million customers in North Carolina, South Carolina, Florida, Indiana, Ohio and Kentucky, and collectively own approximately 54,800 megawatts of energy capacity. Its natural gas utilities serve 1.7 million customers in North Carolina, South Carolina, Tennessee, Ohio and Kentucky."[2] DEC employs more than 27,000 people and generates approximately $30 billion in annual revenue.

23. As a condition of receiving electric and natural gas services, DEC requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from DEC, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

24. In its privacy policy, DEC states "[w]e maintain administrative, technical and physical safeguards designed to protect personal information against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use."[3]

25. Because of the highly sensitive and personal nature of the information DEC acquires and stores with respect to its customers, DEC, upon information and belief, promises to,

[2] See https://www.duke-energy.com/our-company/about-us (last visited Dec. 23, 2024).
[3] See https://www.duke-energy.com/legal/privacy-policy (last visited on Dec. 23, 2024).

among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, DEC assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

B. The Data Breach and DEC's Inadequate Notice to Plaintiffs and Class Members

27. According to Defendant's Notice, it learned of unauthorized access to its computer systems on or around May 2024, with such unauthorized access having taken place between May 20, 2024, and May 24, 2024.

28. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including last four digits of Social Security number and/or federal tax ID number, account numbers, property or mailing addresses, meter serial numbers, email addresses, and phone numbers of millions of individuals.

29. On or about December 12, 2024, roughly seven months after DEC learned that the Class's Private Information was first accessed by cybercriminals, DEC finally began to notify customers that its investigation determined that their Private Information was acquired.

30. DEC delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information may have been "used" and "obtained" by an unauthorized third party.

31. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

32. Thus, DEC's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

33. In addition, the Notice offers no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing one year of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the Data Breach.

34. DEC had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Plaintiffs and Class Members provided their Private Information to DEC with the reasonable expectation and mutual understanding that DEC would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

36. DEC's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

37. DEC knew or should have known that its electronic records would be targeted by cybercriminals.

C. DEC Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses in Possession of Private Information are Particularly Susceptible.

38. DEC's negligence, including its gross negligence, in failing to safeguard Plaintiffs' and Class Members' Private Information is particularly stark, considering the highly public increase of cybercrime similar to the cyber-attack incident that resulted in the Data Breach.

39. Data thieves regularly target entities like DEC due to the highly sensitive information they maintain. DEC knew and understood that Plaintiffs' and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

40. According to the Identity Theft Resource Center's 2023 Data Breach Report, the overall number of publicly reported data compromises in 2023 increased more than 72-percent over the previous high-water mark and 78-percent over 2022.[4]

41. Despite the prevalence of public announcements of data breach and data security compromises, DEC failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised in this Data Breach.

42. As a national service provider in possession of millions of customers' Private Information, DEC knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences they would suffer if DEC's data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, DEC failed to take adequate

[4] *2023 Annual Data Breach Report*, IDENTITY THEFT RESOURCE CENTER, (Jan. 2024), *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last visited on Dec. 23, 2024).

cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

43. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

44. DEC was, or should have been, fully aware of the unique type and the significant volume of data on DEC's network server(s) and systems and the significant number of individuals who would be harmed by the exposure of the unencrypted data.

45. Plaintiffs and Class Members were the foreseeable and probable victims of DEC's inadequate security practices and procedures. DEC knew or should have known of the inherent risks in collecting and storing the Private Information and the critical importance of providing adequate security for that data, particularly due to the highly public trend of data breach incidents in recent years.

D. DEC Failed to Comply with FTC Guidelines

46. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

47. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[5] The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

48. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

49. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

50. Such FTC enforcement actions include those against businesses that fail to

[5] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Dec. 23, 2024).

adequately protect customer data, like DEC here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

51. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like DEC of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of DEC's duty in this regard.

52. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[6]

53. As evidenced by the Data Breach, DEC failed to properly implement basic data security practices. DEC's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

54. DEC was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[6] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Dec. 23, 2024).

E. DEC Failed to Comply with Industry Standards

55. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

56. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[7]

57. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.
f. Have formal policies for safely disposing of electronic files and old devices.
g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

[7] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Dec. 23, 2024).

58. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[8]

59. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

[8] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Dec. 23, 2024).

F. DEC Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

60. In addition to its obligations under federal and state laws, DEC owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. DEC owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

61. DEC breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. DEC's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

62. DEC negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

63. Had DEC remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

64. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with DEC.

G. As a result of the Data Breach, Plaintiffs and Class Members Are at a Significantly Increased Risk of Fraud and Identity Theft.

65. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[9] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

[9] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, FEDERAL TRADE COMMISSION (Oct. 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Dec. 23, 2024).

66. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

67. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

68. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

69. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

70. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

71. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

72. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

73. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[10] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

74. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

75. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

76. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[11] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

77. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[10] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, *available at*: https://www.identitytheft.gov/Steps (last visited on Dec. 23, 2024).

[11] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. DEP'T OF JUSTICE (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited on Dec. 23, 2024).

credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[13]

78. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[14]

79. The Dark Web Price Index of 2023, published by PrivacyAffairs, shows how valuable just email addresses alone can be, even when not associated with a financial account: [15]

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited on Dec. 23, 2024).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last visited on Dec. 23, 2024).

[14] *See Dark Web Price Index: The Cost of Email Data*, MAGICSPAM, https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Dec. 23, 2024).

[15] *See Dark Web Price Index 2023*, PRIVACY AFFAIRS, https://www.privacyaffairs.com/dark-web-price-index-2023/ (last visited on Dec. 23, 2024).

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

80. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

81. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including DEC, collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[16]

82. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[17]

83. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

84. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting

[16] *See Privacy Policy*, ROBINHOOD, https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Dec. 23, 2024).

[17] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

85. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

86. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[18] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[19]

87. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

---

[18] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on Dec. 23, 2024).

[19] *Id* at pp 21-25.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Dec. 23, 2024).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

88. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

89. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

V. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

Plaintiff Kelli Gipson's Experience

90. When Plaintiff Gipson first became a customer, Defendant required that she provide it with substantial amounts of her PII.

91. On or about December 12, 2024, Plaintiff Gipson received the Notice informing her that her Private Information had been "obtained" and/or "acquired" during the Data Breach. The Notice provided that the Private Information compromised included her name, date of birth, last four digits of Social Security number and/or federal tax ID number, account numbers, property or mailing addresses, meter serial numbers, email addresses, and phone numbers.

92. The Notice offered Plaintiff Gipson only year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Gipson will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

93. Plaintiff Gipson suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

94. Plaintiff Gipson would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

95. Plaintiff Gipson suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

96. Plaintiff Gipson suffered actual injury in the form of damages to and diminution in the value of her personal information – a form of intangible property that Plaintiff Gipson entrusted to Defendant for the purpose of receiving electric services from Defendant and which was compromised in, and as a result of, the Data Breach.

97. Plaintiff Gipson suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

98. Plaintiff Gipson has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information

99. As a result of the Data Breach, Plaintiff Gipson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Gipson has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

100. As a result of the Data Breach, Plaintiff Gipson has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Gipson is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

101. Plaintiff Gipson also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Gipson; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

102. As a result of the Data Breach, Plaintiff Gipson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Alyssa Gaseor's Experience

103. When Plaintiff Gaseor first became a customer, Defendant required that she provide it with substantial amounts of her PII.

104. On or about December 12, 2024, Plaintiff Gaseor received the Notice informing her that her Private Information had been "obtained" and/or "acquired" during the Data Breach. The Notice provided that the Private Information compromised included her name, date of birth, last four digits of Social Security number and/or federal tax ID number, account numbers, property or mailing addresses, meter serial numbers, email addresses, and phone numbers.

105. The Notice offered Plaintiff Gaseor only year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Gipson will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

106. Plaintiff Gaseor suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

107. Plaintiff Gaseor would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

108. Plaintiff Gaseor suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

109. Plaintiff Gaseor suffered actual injury in the form of damages to and diminution in the value of her personal information – a form of intangible property that Plaintiff Gaseor entrusted

to Defendant for the purpose of receiving electric services from Defendant and which was compromised in, and as a result of, the Data Breach.

110. Plaintiff Gaseor suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

111. Plaintiff Gaseor has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information

112. As a result of the Data Breach, Plaintiff Gaseor made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Gaseor has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

113. As a result of the Data Breach, Plaintiff Gaseor has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Gaseor is very concerned about this

increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

114. Plaintiff Gaseor also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Gaseor; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

115. As a result of the Data Breach, Plaintiff Gaseor anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

116. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

117. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

118. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

119. As a direct and proximate result of DEC's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

120. Further, as a direct and proximate result of DEC's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

121. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

122. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

123. Plaintiffs and Class Members also lost the benefit of the bargain they made with DEC. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to DEC was intended to be used by DEC to fund adequate security of DEC's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

124. Additionally, as a direct and proximate result of DEC's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

125. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[22]

127. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

128. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiffs and Defendant included

[21] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on Dec. 23, 2024).

[22] *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Dec. 23, 2024).

Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiffs and Class Members did not get what they bargained for.

129. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Addressing their inability to withdraw funds linked to compromised accounts;

c. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

d. Contacting financial institutions and closing or modifying financial accounts;

e. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

130. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of DEC, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

131. As a direct and proximate result of DEC's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

VI. CLASS ACTION ALLEGATIONS

132. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

133. Specifically, Plaintiffs propose the following Nationwide Class definition (collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

134. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

135. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses before the Court determines whether certification is appropriate.

136. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

137. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of millions of customers of DEC whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through DEC's records, Class Members' records, publication notice, self-identification, and other means.

138. **Commonality.** There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether DEC engaged in the conduct alleged herein;

b. When DEC learned of the Data Breach;

c. Whether DEC's response to the Data Breach was adequate;

d. Whether DEC unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether DEC failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether DEC's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether DEC's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether DEC owed a duty to Class Members to safeguard their Private Information;

i. Whether DEC breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether DEC had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether DEC breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether DEC knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of DEC's misconduct;

o. Whether DEC's conduct was negligent;

p. Whether DEC's conduct was *per se* negligent;

q. Whether DEC was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

139. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

140. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

141. **Predominance.** DEC has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from DEC's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

142. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for DEC. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

143. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). DEC has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

144. Finally, all members of the proposed Class are readily ascertainable. DEC has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by DEC.

VII. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class)

145. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

146. DEC knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

147. DEC's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

148. DEC knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. DEC was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

149. DEC owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. DEC's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

150. DEC's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

151. DEC's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

152. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and DEC owed them a duty of care to not subject them to an unreasonable risk of harm.

153. DEC, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within DEC's possession.

154. DEC, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

155. DEC, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

156. DEC breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

157. DEC acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

158. DEC had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust DEC with their Private Information was predicated on the

understanding that DEC would take adequate security precautions. Moreover, only DEC had the ability to protect its systems (and the Private Information that it stored on them) from attack.

159. DEC's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exposed as alleged herein.

160. As a result of DEC's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

161. DEC's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

162. As a result of DEC's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

163. DEC also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

164. As a direct and proximate result of DEC's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

165. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

166. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

167. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring DEC to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class)

168. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

169. Pursuant to Section 5 of the FTCA, DEC had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

170. DEC breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

171. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

172. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of DEC's duty in this regard.

173. DEC violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

174. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to DEC's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

175. DEC's violations of the FTCA constitute negligence *per se*.

176. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to DEC's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

177. As a direct and proximate result of DEC's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

178. DEC breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

179. As a direct and proximate result of DEC's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

180. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring DEC to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

181. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

182. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to DEC in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

183. DEC's Privacy Policy memorialized the rights and obligations of DEC and its customers. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

184. In the Privacy Policy, DEC commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

185. Plaintiffs and Class Members fully performed their obligations under their contracts with DEC.

186. However, DEC did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore DEC breached its contracts with Plaintiffs and Class Members.

187. DEC allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, DEC breached the Privacy Policy with Plaintiffs and Class Members.

188. DEC's failure to satisfy its confidentiality and privacy obligations resulted in DEC providing services to Plaintiffs and Class Members that were of a diminished value.

189. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

190. As a direct and proximate result of DEC's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

191. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring DEC to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

192. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

193. This Count is pleaded in the alternative to Count III above.

194. DEC provides electric utility and natural gas services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services from Defendant.

195. Through Defendant's sale of services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with DEC's policies, practices, and applicable law.

196. As consideration, Plaintiffs and Class Members paid money to DEC and turned over valuable Private Information to DEC. Accordingly, Plaintiffs and Class Members bargained with DEC to securely maintain and store their Private Information.

197. DEC accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

198. In delivering their Private Information to DEC and paying for services, Plaintiffs and Class Members intended and understood that DEC would adequately safeguard the Private Information as part of that service.

199. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

200. Plaintiffs and Class Members would not have entrusted their Private Information to DEC in the absence of such an implied contract.

201. Had DEC disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to DEC.

202. DEC recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

203. DEC violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

204. Plaintiffs and Class Members have been damaged by DEC's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

205. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

206. This Count is pleaded in the alternative to Counts III and IV above.

207. Plaintiffs and Class Members conferred a benefit on DEC by turning over their Private Information to Defendant and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

208. Upon information and belief, DEC funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

209. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with

applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to DEC.

210. DEC has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

211. DEC knew that Plaintiffs and Class Members conferred a benefit upon it, which DEC accepted. DEC profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

212. If Plaintiffs and Class Members had known that DEC had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

213. Due to DEC's conduct alleged herein, it would be unjust and inequitable under the circumstances for DEC to be permitted to retain the benefit of its wrongful conduct.

214. As a direct and proximate result of DEC's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

(v) the continued risk to their Private Information, which remains in DEC's possession and is subject to further unauthorized disclosures so long as DEC fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

215. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from DEC and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by DEC from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

216. Plaintiffs and Class Members may not have an adequate remedy at law against DEC, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class)

217. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

218. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described in this Complaint.

219. DEC owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

220. DEC still possesses Private Information regarding Plaintiffs and Class Members.

221. Plaintiffs allege that DEC's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

222. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. DEC owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. DEC's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. DEC continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

223. This Court should also issue corresponding prospective injunctive relief requiring DEC to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order DEC to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, DEC must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on DEC's systems on a periodic basis, and ordering DEC to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of DEC's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps DEC's customers should take to protect themselves.

224. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at DEC. The risk of another such breach is real, immediate, and substantial. If another breach at DEC occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

225. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to DEC if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of DEC's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and DEC has a pre-existing legal obligation to employ such measures.

226. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at DEC, thus preventing future injury to Plaintiffs and other customers whose Private Information would be further compromised.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing DEC to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring DEC to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: December 23, 2024.

Respectfully submitted,

/s/ Dana Smith

Dana Smith, Bar No. 51015
Tyler J. Bean
Gabrielle Williams
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: dsmith@sirillp.com
E: tbean@sirillp.com
E: gwilliams@sirillp.com

Attorneys for Plaintiffs and the Putative Class